ARCTIC WOLF

JUNE 2026

State of the Cybersecurity Attack Surface

INSIGHTS FROM AURORA® EXPOSURE MANAGEMENT

TABLE OF CONTENTS

Executive Summary

As an industry, we have become remarkably proficient at identifying high-severity CVEs, but acting on vulnerabilities and a broader set of exposures is a greater challenge. Patch cycles routinely stretch into weeks or months, and the gap between knowing, prioritizing, and fixing is where risk accumulates within enterprise environments.

We know that seeing an exposure and doing something about it are two very different things.

And the vulnerability remediation gap is only part of the picture. Beyond traditional CVEs, subtler and more pervasive classes of risk continue to grow within the everyday processes that enterprises rely on to operate.

Misconfigurations, known vulnerabilities lacking context, missing or disabled controls, identity-based risk, unmanaged assets, end-of-life software, and access that is far broader than it should be all contribute to a landscape of risk that security teams don't always see, but are still accountable for. These exposures rarely drive headlines the way high-profile CVEs do, but the danger is just as impactful.

This urgency is intensifying, and the modern attacker is exploiting it from both ends. In the 2026 Arctic Wolf Threat Report, 65% of non-business –email compromise (BEC) incident response cases involved abuse of external remote access services such as RDP, VPN, and RMM tools, and the top 10 most frequently exploited vulnerabilities all had patches available — no zero-days required. Attackers are finding the same forgotten, unprotected, and unpatched assets that leave the door to your crown jewels open. At the same time, frontier AI is evolving the attacker toolkit, accelerating reconnaissance, lateral movement, and targeting. Emerging surfaces like MCP servers and over-provisioned AI agent access are widening the blast radius of every gap.

This State of Attack Surface Management report draws on aggregated, anonymized data from Aurora® Attack Surface Management, part of the Aurora Exposure Management portfolio, representing visibility into more than 800,000 IT assets. The findings show enterprises remain dangerously exposed to traditional vulnerabilities, configuration gaps, missing controls, and identity-based risk.

KEY FINDING:

Across the data set, 18% of IT assets are not covered by enterprise patch or configuration management, 10% are missing endpoint protection, and 19% have reached end-of-life. These are not edge cases. They represent the reality of the modern attack surface.

In 2026, the organizations that set themselves apart and meaningfully lower their breach potential will be those investing in proactive cyber risk management programs and strategies, not just faster reactions to the latest CVE. This report quantifies the scale of the problem, explains how broad exposure manifests in real enterprise environments, and offers a path forward built on continuous visibility, security-grade asset intelligence, and verified remediation.

Dan Schiappa
Chief Product and Services Officer
Arctic Wolf

Key Takeaways

Exposures are widespread, leaving enterprise networks at risk

Configuration Misses: Across more than 800,000 IT assets, 18% are not covered by enterprise patch or configuration management, creating environments where known weaknesses cannot be reliably remediated.

Control Gaps: 10% of IT assets are missing endpoint protection, giving attackers a direct path into enterprise networks.

Invisible Vulnerabilities: More than 17% of IT assets are not visible to legacy vulnerability management solutions, meaning they are never scanned for the CVEs that threat actors are actively exploiting.

End-of-life assets have become a structural risk, not an exception

Aurora Attack Surface Management data shows end-of-life assets are concentrated in the systems organizations rely on most: **legacy servers, virtualized infrastructure, and shared end-user devices.**

19% of IT assets have reached end-of-life, running hardware or software that no longer receives vendor security updates. These devices are a structural risk.

Attackers do not need zero-days when so much is unguarded

65% of non-BEC incident response cases involved abuse of remote access services such as RDP, VPN, and RMM tools. Every one of the 10 most frequently exploited CVEs dates from 2024 or earlier and had a patch available.

>8X
INCREASE

As patching of internet-facing systems has improved, **trusted-relationship and misconfiguration abuse surged from under 1% to 8%** of non-BEC IR cases — a textbook example of attackers pivoting to wherever environmental visibility is weakest.

The State of the Cybersecurity Attack Surface

Exposures are ramping up, and the gaps are growing

IT assets missing at least one critical control represent a class of exposure sitting in the blind spot of security teams. That includes assets missing endpoint security (i.e. endpoint protection or detection and response) and assets not covered by enterprise patch or configuration management tooling.

18%
of IT assets are not covered by enterprise patch or configuration management

10%
of IT assets are missing endpoint security

17%
of IT assets are not covered by enterprise vulnerability management

Taken together, these findings describe an enterprise attack surface where foundational controls are not where they need to be. One in three IT assets (33%) is missing at least one of these critical controls, meaning the asset exists in a blind spot outside processes and best practices widely treated as baseline security hygiene.

The endpoint security gap deserves more attention than its size suggests. Modern threat campaigns increasingly rely on living-off-the-land techniques where attackers abuse legitimate enterprise tools instead of dropping noisy, detectable malware. The single most effective defense against this trend is endpoint detection and response. An asset without it becomes an extremely valuable tool to an attacker for lateral movement, credential theft, persistence, and ransomware deployment. With nearly one in 10 assets running without endpoint security (i.e. protection or detection and response tooling), attackers are given ample opportunity to exploit this weakness.

Security leaders consistently cite vulnerability management as a primary technology investment area, yet attack surfaces remain riddled with a broader set of exposures. Four structural problems define why asset inventory is so difficult today:

- **Organizational structures:** Most enterprises separate the teams responsible for maintaining assets (IT) from the teams accountable for securing them (Security). Coverage breaks down at that handoff, and incomplete data and outdated records can worsen critically important visibility.
- **Attack surface growth:** Hybrid infrastructure, distributed workforces, AI adoption, and cloud growth have outpaced every team's ability to maintain a single, current view.
- **Multiple incomplete inventories:** Every tool has its own list of assets, and none of them are complete on their own.
- **Siloed data with no reconciliation:** Without continuous correlation across sources, gaps and duplicates accumulate and hide real exposure.

The downstream effect: Devices and servers that are not in patch management may have known CVEs, but they are not getting patched. Assets not identified in vulnerability management are never scanned. Assets without endpoint security give attackers a direct path in. Most enterprises understand they should patch the assets they know about. But a lack of prioritization and a list of unknown assets introduce invisible risk that often give bad actors the upper hand.

Every one of the top 10 CVEs most frequently exploited in Arctic Wolf's 2025 non-BEC incident response cases dates from 2024 or earlier, and the most common (CVE-2024-40766, a SonicWall SonicOS access control vulnerability) had a patch available well before it was abused at scale. The challenge is not that vendors have not issued fixes. The challenge is that organizations cannot see, prioritize, or verify deployment on the assets that need them.

Beyond CVE Scoring: Vulnerabilities Demand Context to Determine Risk

The most frequently exploited vulnerabilities found in Arctic Wolf's incident response cases are not novel zero-days, but known, patchable flaws concentrated in a small set of high-value internet-facing and/or edge technologies. Two trends define the list:

01

First, every entry includes an internet-facing appliance that sit at the perimeter. These assets often fall outside the coverage of endpoint security and vulnerability management tooling, and are the types of blind spots bad actors prioritize from the outside in.

02

Second, the vulnerabilities are not new. The list spans CVEs from 2024 back to a 2021 Microsoft Exchange cluster. The single most exploited entry, SonicWall Sonic OS CVE-2024-40766, had a patch available well before it was exploited at scale.

Edge devices are inherently risky due to the nature of their internet-facing position. But they also accelerate adversary progression through the kill chain. Because edge appliances inherently grant elevated access, exploiting one frequently lets an attacker skip the privilege escalation phase entirely. This is why prioritization, not patch volume, is the practice and behavior that matters. Not all vulnerabilities are created equal. A medium-severity authentication bypass on an internet-facing appliance can represent far greater real-world risk than a critical-rated vulnerability on an internal, well-segmented asset. A program driven by CVSS scores alone would confuse that priority, leaving an organization exposed to a higher likelihood of breach.

Effective exposure management combines threat intelligence, business context, and asset intelligence to surface the handful of exposures that have the potential to cause the most disruption. Once identified, automated remediation workflows and one-click mitigations make it possible to act, verify, and fix exposures without the manual overhead that lets known exposures linger for weeks and months.

Vulnerability Landscape Evolution

AI is accelerating vulnerability discovery for researchers and adversaries alike, and this dynamic collides directly with the coverage gap described earlier in this report. When nearly one-fifth of the environment (17%) is never scanned for known CVEs, those assets are exposed to threat dynamics moving faster than manual vulnerability management processes can accommodate.

The compression is happening in two categories. Initiatives like Anthropic's Claude Mythos model and Google's Big Sleep project have separately shown LLM-driven tooling identifying novel flaws in critical infrastructure in minutes and hours rather than weeks and months. AI-assisted discovery is shortening the time for defenders to react to a vulnerability becoming known and a working exploit existing. At the same time, as the cost of generating exploits lowers, vulnerabilities that have sat dormant for years become more economical to attack. In this reality, prioritization that tells teams what to fix first becomes a critical capability.

End-of-Life Assets: A Ticking Time Bomb

Trusted systems that have been in production for more than a decade are prime targets for exposures. Hardware, software, and OT/IoT devices reach end-of-life, and when they do, the vendor stops issuing security updates. Whatever vulnerabilities exist on those systems will remain there, forever, until the asset is removed from the network.

of IT assets across the data set have reached end-of-life

Nearly one in five IT assets are running hardware or software that no longer receives vendor security updates. Several scenarios are converging including aging Windows Server and Windows 10 endpoints reaching unsupported status, virtualized infrastructure outliving its support window, and IoT and operational technology devices that were never on a patch lifecycle in the first place.

End-of-life systems are low-hanging fruit for threat actors. They are easy to exploit using existing, proven techniques, and they often sit in parts of the environment most connected to sensitive data. The low-effort, high-yield combination exists alongside a broader pattern in the 2026 Arctic Wolf Threat Report where we describe attackers "logging in instead of breaking in," abusing remote access tools and exploiting a small set of known, patchable vulnerabilities concentrated in exposed edge technologies. When the door is unpatched or unable to be patched, the entry technique is identical.

There are situations where end-of-life systems are unavoidable. A clinical application that only runs on a legacy operating system, or an industrial control system whose vendor is long out of business, may need to remain in place. The point is not that every end-of-life asset should be ripped out tomorrow, that's not recommended. It is that security teams need to know they exist, what protections are in place around them, and what compensating controls are required to lower the likelihood and impact of an attack.

Beyond the Data: Exposures in the Wild

The following real-world examples from an Aurora Attack Surface Management case study show how exposures manifest in real-world environments, and how a continuous, risk-aware view of the attack surface helps teams close them.

Remote access exposures hiding inside the trusted network

The 2026 Arctic Wolf Threat Report found that 65% of non-BEC IR cases involved abuse of remote access tools, a steady climb from just 24% three years ago. That same pattern shows up as legacy VPN concentrators, forgotten RMM agents on retired endpoints, and remote access services running on systems with stale or missing endpoint protection. Aurora Attack Surface Management surfaces those exposures by correlating remote access services with control coverage, end-of-life status, and asset context, giving teams the visibility needed to remove or harden the paths attackers are most likely to use.

Aging operating systems and incomplete migrations

As IT and security teams dig into their asset inventories with Aurora Attack Surface Management, many discover operating systems and servers they did not believe were still in the environment. While the aggregate data set shows 19% of IT assets at end-of-life, that number is often higher inside individual organizations.

When one enterprise deployed Aurora Attack Surface Management, the team identified that more than 14% of IT assets had reached the end-of-life stage, including instances of Windows Server 2008 R2, Windows Server 2012, and desktop operating systems going back to Windows 7. These end-of-life systems sat in critical areas of the business, running applications that the organization had assumed were already migrated.

Limited visibility into migrations

Identifying vulnerable assets and migrating them to a supported OS can be a manual and arduous process.

The same organization mentioned above later underwent a large migration to retire its end-of-life systems. Security mandated that individual business units roll out the upgrade. The business units confirmed completion. There was no independent process to verify the mitigating action. A subsequent Aurora Attack Surface Management scan revealed a 41% improvement in devices that had reached end-of-life, but 8% of assets remained end-of-life despite business unit confirmation.

Without Aurora Attack Surface Management, there was no way to know the migration was incomplete. This is one of the most consistent patterns we see: Mandating a migration and relying on the people responsible for executing it to also confirm completion creates a false sense of security.

Inaccurate sources of truth for endpoint protection

When the same customer attempted to verify that all its IT assets were covered by endpoint protection, exposures made accurate verification impossible. The customer's configuration management tool reported full coverage. An Aurora Attack Surface Management scan showed that 2% of enterprise endpoints were absent from the configuration management system entirely. The single source of truth was wrong, and the security team had been operating on a false sense of coverage.

THE LESSON:

Single-tool inventories cannot be trusted as a sole source of truth. Continuous, multi-source correlation is what reveals the gaps individual tools cannot see.

Sector concentration: modern organizations relying on legacy systems

The 2026 Arctic Wolf Threat Report identified manufacturing as the most successfully attacked sector on ransomware leak sites, with nearly 70% more victims than the second-place sector. Manufacturing is also where Aurora Attack Surface Management consistently surfaces high concentrations of exposures: engineering and production workstations sitting outside standard patch management, aging operating systems kept in place to support long-lived equipment, and remote access tools deployed for vendors and third parties that were never decommissioned.

The same pattern holds in other sectors that pair sustained attacker interest with deep legacy footprints.

- Healthcare ranks among the most frequently targeted sectors in both Arctic Wolf's ransomware incident response cases and ransomware leak-site data. Clinical and diagnostic systems frequently run on operating systems well past end-of-life. These systems often sit close to sensitive patient data while falling outside enterprise patch and endpoint security coverage. Aurora Attack Surface Management helps security teams identify end-of-life endpoints and servers that may have been assumed retired or protected.
- Banking, financial services, and insurance (BFSI) organizations rank among the most heavily targeted sectors, marked by decades-old core banking and transaction systems, layered acquisitions, and a dense web of third-party and remote-access connections. Aurora Attack Surface Management surfaces an accurate, continuously reconciled view of which assets exist, which are covered, and which remote-access paths remain active.

"In multiple investigations this year, we observed attackers achieve domain-level control in minutes. That speed leaves little room for manual intervention and underscores why continuous monitoring and rapid response are increasingly viewed as essential."

Kerri Shafer-Page, VP of Incident Response, Arctic Wolf, 2026 Arctic Wolf Threat Report

Why Security Teams Prioritize Exposure Management

Three trends are pushing an exposure management strategy further into the foreground.

01

The attack surface is expansive by nature

Modern environments stretch across internal infrastructure, cloud workloads, SaaS, external-facing services, identities, unmanaged endpoints, and operational technology. AI is influencing greater growth as enterprise environments build more, faster. Each layer comes with its own inventory tools, none of which see the full picture and lack contextual awareness. Without continuous visibility, real-time assessment, and accurate deduplication, the aggregate inventory drifts from reality every day.

02

Attackers favor the path of least resistance

The same small set of known, patchable vulnerabilities described earlier — all dating from 2024 or before — continues to account for most vulnerability-driven intrusions. Alongside them, 65% of non-BEC IR cases came from abuse of remote access tools, a steady climb from 24% three years ago, and data-only extortion incidents grew 11x year over year, jumping from 2% to 22% of all IR cases. Attackers are still finding success with old techniques, and AI is speeding those old techniques up.

As organizations have improved their patching of internet-facing systems, the share of IR cases driven by external exploits has dropped from 29% to 11%. Over the same period, abuse of remote access services has more than doubled, and the share of cases caused by trusted-relationship abuse and misconfigurations has surged from under 1% to 8%. As defender behavior has matured, attackers have redirected efforts toward whatever exposure is least defended. That is precisely the kind of gap an organization cannot close without

03

Cyber risk has evolved into a business and board-level responsibility

Cybersecurity programs are increasingly measured through audit findings, cyber insurance eligibility, regulatory disclosure obligations, and board-level risk reporting. Each of these depends on an organization's ability to state, with confidence, what it has and how well it is protected. An inaccurate asset inventory influences a greater degree of cyber and regulatory risk. When coverage gaps surface after an incident, the cost is not exclusive to remediation. Failed audits, fines, higher premiums or denied claims, disclosure exposure, and eroded trust come with significant monetary loss. Exposure management turns "we think we're secure" into "we can prove we're secure," which is the new standard businesses are held to.

THE BOTTOM LINE:

Visibility is no longer a one-time project. It is the foundation that every other security investment depends on. When 33% of assets are missing a critical control and 19% are end-of-life, the most expensive part of a security program is operating without an accurate map.

The data also revealed a clear maturity gradient. Across every exposure category we measured, organizations with established Aurora Attack Surface Management deployments showed materially better coverage than those earlier in their journey.

Instances of missing configuration management and missing endpoint security fell by 43%

Vulnerability management coverage gaps dropped by more than 40%

End-of-life exposure declined by nearly 45%

Exposure is not a fixed condition. It improves considerably as programs mature, visibility deepens, and remediation speeds up through workflow automation and one-click patching. And while attack surfaces keep growing and shifting, exposure management ensures new risk factors are captured in real time before they have an opportunity to be exploited.

Conclusion

Security teams need to understand which exposures matter in a broader context, and whether they ever get fixed.

Prioritization built on severity scores alone is closer to guesswork than strategy, and while a CVSS rating is helpful in theory, it doesn't account for broader cybersecurity risks and exposures or your specific environmental context. Without asset intelligence, business context, and threat intelligence enrichment teams end up focusing on the wrong risks.

The findings in this report show visibility into the attack surface remains incomplete. Closing this gap requires a continuous, proactive approach to see everything and focus on what matters. Critically, it requires the ability to see vulnerabilities, misconfigurations, and other exposures in context with one another.

A missing control on a critical, internet-facing asset is a different problem than the same gap on an isolated test machine. Prioritization that combines threat intelligence, exploitability, asset criticality, and business context is what separates a list of findings from a plan of action. And it requires built-in remediation workflows that make it easy to mitigate and verify actions to eliminate cyber risk.

This is what Aurora Exposure Management was built for. By providing continuous visibility across surfaces, accurate asset inventories, prioritization, and remediation verification, security teams unlock the foundation they need to manage exposures at scale and to mature toward a continuous threat exposure management program. By aggregating and correlating asset data across the security and IT tools cybersecurity teams already use, Aurora Attack Surface Management uncovers what individual tools cannot: where the most meaningful gaps exist, and which ones matter the most.

The payoff is staying out of the sight line of bad actors. Our platform approach is designed to provide real-time visibility and context-driven prioritization, which helps to find and address exposures before an attacker has an opportunity to exploit them. Proactive teams set the standard, while reactive teams inherit the risk. The organizations that will meaningfully reduce risk are the ones that recognize that visibility, control coverage, and remediation verification are cornerstones of a modern security strategy.

The organizations that will reduce risk fastest are the ones that stop treating asset visibility as a side project. They are the ones that recognize visibility, control coverage, and remediation verification as the operational core of a modern security program. Aurora Attack Surface Management is how that program begins.

> **"The strongest negotiating position is resilience. When recovery does not depend on an attacker, the economics of extortion shift in favor of the defender."**
>
> *Ismael Valenzuela, VP of Labs, Threat Intelligence, Arctic Wolf, 2026 Arctic Wolf Threat Report*

Methodology and Glossary

Methodology

Data in this report is drawn from aggregated, anonymized Aurora Attack Surface Management customer and prospect environments. The data set represents visibility into more than 800,000 IT assets across organizations of varying size, geography, and industry. All findings are de-identified and reported in aggregate.

Glossary

- **IT asset:** A device collected from an inventory source in a customer environment and correlated with devices collected from other sources to produce a unified asset inventory.
- **Exposure:** Any vulnerability or gap in the configuration or state of an IT environment, including missing controls, unknown or unmanaged assets, and end-of-life software. In this report, the term primarily refers to IT assets missing at least one critical control: endpoint protection or patch and configuration management.
- **Source:** An inventory source in the customer environment that provides information about devices, users, software, or controls.
- **Stale records:** Devices that continue to appear in one inventory source (such as endpoint protection) but are not identified in any other source, and whose agent has not reported in for more than 30 days.
- **End-of-life device:** A device running hardware or software that no longer receives security updates from the vendor.